NetCompetition's Comments on the FCC's Title II Privacy NPRM

MB Docket No. 16-106

Note: Comments are from Scott Cleland, Chairman of NetCompetition, a pro-competition e-forum representing broadband interests. **See** www.netcompetition.org**.**

NetCompetition FCC Comments: The 7 Huge Flaws in the FCC's Proposed Title II Privacy Rules

Summary: It is rare for an FCC proceeding to be so wrong-headed and ill-conceived that it has seven huge flaws. Tellingly this one does.

1. The FCC is trying to force-fit inherently-irreconcilable, telephone closed-ecosystem privacy rules into a broadband open-system Internet.
2. There is no way for an average consumer to understand what part of their privacy is or is not now protected when by the FCC and what part is or is not protected when by the FTC.
3. The FCC's Title II decision was perversely subtractive in eliminating all FTC broadband consumer privacy protections, during the year-plus period while the FCC tries to figure out what FCC consumer privacy protections will replace the FTC's.
4. Since the FCC regulates broadband ISPs, but not edge providers' use of consumer network information, the FCC has managed to provide consumers with unequal privacy protection, and companies with unequal commercial opportunity.
5. The FCC proposes to regulate the biggest privacy risk platforms the least.
6. Google, which is the edge platform that collects the most consumer private information by far, expects no FCC regulation at all.
7. FCC justification for regulating ISPs and not edge providers, because it is hard to switch ISPs, does not equally consider how difficult it is to leave the omnipresent and persistent tracking of Google, even if one leaves all of their services.

The full explanations of these huge flaws are explained in detail in the seven analyses of the FCC's proposed privacy regulations below.

1. PrecursorBlog: Why FCC Title II Telephone Privacy Rules Can't Work with an Open Internet

Submitted by Scott Cleland on Wed, 2016-01-27 10:22

Square peg meet round hole.

The FCC is poised to try and force-fit inherently-irreconcilable, telephone closed-ecosystem privacy rules into a broadband open-system Internet. Good luck with that.

Expect the FCC to have fits trying to successfully craft workable, non-arbitrary, and legally-sustainable Title II broadband privacy rules in the year ahead.

It is a problem of the FCC's own making.

In arbitrarily applying Title II telecommunications rules to only the ISP half of Internet communications, while politically exempting the entire edge half of Internet communications in its Open Internet order, the FCC has ensured that information that was proprietary and controllable in the closed telephone world becomes public and uncontrollable in the open Internet world.

Horses meet open barn door.

Net neutrality activists wrongly imagined that Title II was all-purpose-regulatory-authority to impose "the strongest possible" Open Internet rules they wanted, like bans on paid prioritization, zero rating or usage based pricing, despite decades of Title II and court precedents that determine many types of economic price discrimination and pricing flexibility to be just and reasonable.

Now they appear to be imagining wrongly again that Title II Section 222 "*Confidentiality of Customer Proprietary Network Information*" will somehow be strong all-purpose-privacy-authority to impose whatever privacy rules they want, when in reality Section 222 is specific and limited telephone confidentiality authority, that depends entirely on a closed telephone ecosystem for its success, and that is antithetical to the FCC's Open Internet ecosystem predicate.

There is a reason the term and concept of a "wiretap" exists.

The traditional telephone system was by design a closed and highly secure ecosystem and technology. If the government wanted access to people's private calling information or the content of a call for law enforcement or national security purposes, they needed a court authorized warrant or order to physically tap a telephone wire.

There also is good reason the term and concept of "data breach" is so common and widely-known.

The Internet was designed to be open, not closed, private or secure.

The Internet's co-designer, Vint Cerf, **explained** in a 2009 interview why. *"It's true that we didn't focus very heavily on the security side at the time that we were finalizing the current protocols that you're using. We were much more concerned about whether it worked at all, as opposed to, "does it work securely?""*

He further explained in a 2008 **interview**: *"The idea of a virtual private network was not part of the original design. It was actually an oversight. It didn't occur to me that it would be useful until afterwards.*"

When asked about Internet security in general, Mr. Cerf candidly **explained**: *"It's every man for himself. In the end, it seems every machine has to defend itself. The internet was designed that way."*

Ironically, the Internet's co-designer and Google's Internet Evangelist, Vint Cerf, believes that the primary privacy and security problem by design on the Internet are edge devices/providers -- not ISPs.

Enter net neutrality activists, stage left on cue.

Recently, sixty net neutrality activist organizations urged the FCC in a **letter** to quickly propose a Title II broadband privacy rulemaking to make the FCC "*a brawnier cop on the beat*" on privacy matters.

Just like net neutrality activists politically commanded an FCC majority to impose "bright line" net neutrality rules on the broadband sector without Congressional involvement or authority, the same net neutrality activists now seek to command the FCC majority to impose a new broadband-only Internet privacy policy on the broadband sector without Congressional involvement or sufficient authority.

Expect the most serious privacy advocates to see through this nonsensical, "one-hand clapping" folly and urge the FCC to apply Section 222 more comprehensively, justly and reasonably, to *both* sides of communications, i.e. ISPs *and* edge providers.

The problem is it is way too late for that.

The FCC probably doomed Title II Section 222 rules to failure when it arbitrarily asserted that the open Internet and the Public Switched Telephone Network (PSTN) were one in the same in the Open Internet order, and when they also arbitrarily exempted the edge downstream half of communications from Title II reclassification, apparently at the command of a last minute **ex parte filing** from Google.

Consider the untenable prospect of imposing only on broadband providers a duty to keep Customer Proprietary Network Information (CPNI), confidential when under net neutrality rules they are not allowed to block Internet traffic that automatically may transmit "confidential" CPNI to the public via the purveyors of browsers, operating systems and apps, which by the way, have no duty on the other side of the communications to keep the users' CPNI confidential and not use it for commercial purposes without permission of the customer.

Simply, Internet users' CPNI is what edge platforms and Big Data companies routinely use by design to track, profile, and monetize user private information to fund free content on the open Internet.

How could FCC broadband privacy rules ultimately be considered "just and reasonable" under Title II if they put an ISP in an impossible compliance situation, where they can't block or filter traffic to ensure the confidentiality of CPNI under the FCC's net neutrality bright line bans in the Open Internet order, but they still are subject to privacy enforcement action for not fulfilling their duty to protect the confidentiality of CPNI, when it's the design of the open Internet and the open expectations of net neutrality that make CPNI confidentiality almost impossible to protect?

In sum, net neutrality activists have bullied the FCC majority into an untenable situation where they apparently can't justly and reasonably hold only one side of Internet communications accountable for protecting a user's privacy on the Internet, when it fosters open Internet policies that exempt the other side of Internet communications by edge providers from any accountability to protect users' CPNI confidentiality.

Think of this problem as a proverb; the judge (FCC) can't justly and reasonably hold a farmer legally culpable for letting a horse escape a barn, if the judge (FCC) previously mandated that the farmer's barn can't have walls or tethers to keep the horse inside the barn.

***

2. PrecursorBlog: Consumer Confusion over FCC's Arbitrary Privacy Policymaking

Submitted by Scott Cleland on Mon, 2016-02-15 22:48

What's a consumer to think about what the FCC's responsibility is for their privacy protection?

Let me try to explain to a consumer what the Federal Communications Commission (FCC) arbitrarily has done, and apparently intends to do, for consumer internet privacy protection going forward.

By way of background, for the first decade of the Internet when consumers used dial-up technology, the FCC was responsible for protecting consumers' private network information from commercial use without their permission.

For the second decade of the Internet when consumers came to use broadband technology, the FCC ceded its dial-up-Internet privacy protection authority to the Federal Trade Commission (FTC) which became responsible for consumer privacy protection from unfair and deceptive practices consistently across the entire American Internet ecosystem, regardless of who interacted with consumers' private information.

Last spring, in order to assert legal authority to enforce net neutrality to protect edge providers from potential traffic discrimination in the FCC's Open Internet Order, the FCC incidentally clawed back some privacy authority over Internet communications -- over the FTC's strong objections.

To do so, the FCC had to re-imagine and declare that the broadband Internet was the same as the Public Switched Telephone Network for legal purposes, despite one being a predictable, closed-circuit, switched, network and the other being an unpredictable, open packet-switched, routed Internetwork.

At the last minute, and over the best judgment of the FCC's legal team, the FCC ceded to a **petition** from Google, which wanted the FCC to legally split the Internet effectively into different two halves, upstream communications traffic and downstream communications traffic, where the FCC would be responsible

for utility regulation of the upstream communications traffic half of Internet service coming from the consumer to "edge providers" (Google, Facebook, Amazon, etc.), while the FTC apparently would be responsible for the downstream communications traffic half coming from the edge providers to the consumer.

So consumers may need to remember that when they send something to someone on the Internet, their ISP Customer Proprietary Network Information (CPNI), which "*means information that relates to the quantity, technical configuration, type, destination, and amount of use of*" telecommunications, may need to be kept private by their ISP in the future.

At the same time they also need to remember that the edge companies that receive that same upstream traffic which is naturally and inherently filled with CPNI in every communication, have no responsibility from the FCC, or the FTC, to protect the privacy of that CPNI private information.

Thus a helpful rule-of-thumb for consumers to remember about how the FCC's new privacy policy will likely work, is this – whatever is the opposite of common sense.

On one hand the companies that consumers directly pay for their telephone, cellular, Internet access or cable service, whose economic interests are directly aligned with their paying customers, have FCC strict consumer privacy protection responsibilities, like they long have.

However, on the other hand, edge companies -- who are not paid by the consumer, and who collect, track and mine as much private consumer information without their permission as digitally possible to fund their advertising businesses, and who are not economically-aligned with consumers' interests because the consumer is not their customer, but the product they sell to advertisers – will likely have absolutely no FCC or FTC responsibility to protect the privacy of consumers' CPNI.

In addition to having an arbitrary and nonsensical ISP privacy policy, the FCC has signaled that in its upcoming AllVid proceeding, it plans to be consistently arbitrary and nonsensical in also having an arbitrary and nonsensical cable privacy policy for sellers of cable set-top boxes, where on one hand it will protect consumers' video viewing privacy if the consumer gets their cable set-top-box from a regulated cable service or DBS service provider, but not if a consumer buys a similar video-viewing cable set-top-box from Google or another edge provider.

In sum, how is an American consumer to make sense of the FCC's privacy policy now and going forward?

They aren't.

A consumer can discern from the apparent arbitrariness of the FCC's actions to date that this FCC's first purpose is not consumer protection, its first purposes are protecting the FCC's relevance and picking edge business interests as winners over ISP, wireless, cable and DBS provider business interests.

As the old adage goes, watch what they do, not what they say.

***

3. PrecursorBlog: The FCC's New Subtractive Privacy Policy

Submitted by Scott Cleland on Thu, 2016-03-10 19:21

Less is not more. That's real "common sense."

When one's actions demonstrably create a worse rather than better outcome net-net, like the FCC's new Title II ISP privacy policy does, others would justifiably consider it a mistake.

While the FCC obviously complied with President Obama's call for regulating broadband as a Title II utility, the FCC obviously ignored President Obama's 2011 **call** for a 21st century regulatory system, where he said we are "*making it our mission to root out regulations that conflict, that are not worth the cost, or are just plain dumb*."

Let's consider how the FCC's new privacy policy fails this President Obama stated standard for "modern" regulation.

When the FCC reclassified broadband to be a Title II telephone utility last year in its Open Internet **Order**, the FCC trumpeted one of the great net benefits would be increased consumer privacy protection.

Well over a year later, the FCC is just getting around to *proposing* these new Title II privacy protections, and the evidence shows consumers' privacy protection is worse off with the FCC's Open Internet Order.

In their self-serving lust for Title II authority, the FCC cavalierly left American consumers with no ISP privacy protection, i.e. no FTC privacy protection and no "modern" FCC privacy protection. What! How could that nonsensical outcome happen?

When the FCC reclassified broadband as a telephone utility, the FCC willfully triggered the Title II FTC exemption which means that ISPs were not subject to FTC authority, and the FCC made clear that they understood they had to modernize the Title II section 222 CPNI rules because broadband networks are architected completely different than a telephone network and create different list of potential info that could be considered "proprietary."

So American ISP consumers have no privacy protection now and still won't until the FCC passes final rules over eighteen months after the FCC eliminated their FTC privacy protections.

It is telling that neither the FCC nor the FTC have done anything to notify consumers that they have no Internet service privacy protections at all because of their bureaucratic turf war. That's because no consumer could understand such "*regulations that conflict*."

The FCC also knows that their pending section 222 CPNI protections depend on the FCC's Open Internet Order being upheld on appeal in the DC Circuit and the Supreme Court, overall and for wireless, which is

the most at risk legally. If the FCC order is overturned overall, or in part, some or all ISP consumers would have gone without any ISP privacy protection for naught.

The FCC also did not do a cost-benefit analysis as the President's 2011 Executive Order **13563** requires. The FCC was supposed to use "*the least burdensome tools for achieving regulatory ends*," and to "*adopt a regulation only upon a reasoned determination that its benefits justify its costs*." Simply, there is no cost-benefit analysis that these conflicting regulations "*are worth the cost*."

One of the biggest problems with these ISP privacy rules is that are based on a "*just plain dumb*" FCC reclassification legal decision in the FCC's Open Internet order that ensures that the FCC's privacy rules arbitrarily can apply to only one half of the traffic an ISP handles.

That's because at the last minute, and over the best judgment of the FCC's legal team, the FCC ceded to a **petition** from Google, which wanted the FCC to legally split the Internet effectively into different two legal halves, upstream communications traffic and downstream communications traffic, where the FCC would be responsible for utility regulation of the upstream communications traffic half of Internet service coming from the consumer to "edge providers" (Google, Facebook, Amazon, etc.), while the FTC apparently would be responsible for the downstream communications traffic half coming from the edge providers to the consumer.

That's "*just plain dumb*" in any analysis.

In short, these FCC ISP privacy regulations are neither additive, nor "common sense" as the FCC claims.

Sadly, they actually are subtractive, in that they violate the President's regulatory "*mission to root out regulations that conflict, that are not worth the cost, or are just plain dumb*."

***

4. PrecursorBlog: FCC Unequal ISP Privacy Policy Is Unequal Protection & Unequal Opportunity

Submitted by Scott Cleland on Thu, 2016-03-31 16:05

The FCC's just-passed, 3-2 unequal ISP privacy policy spotlights how badly the FCC has lost its way.

In prioritizing the equality rights of inanimate digital bits above the equal protection and equal opportunity rights the American people enjoy under our constitutional republic, the FCC is discriminating in favor of open cronyism over equal consumer protection and equal competitive opportunity.

Moody's Investors Service has done everyone a service in **exposing** the FCC's Title II reclassification and privacy policy for what it really is – arbitrary unequal treatment under the law.

When the FCC proposed these ISP privacy rules three weeks ago, Moody's called the FCC's proposal as it saw it in a **Sector Comment** March 14 entitled: "*FCC's broadband privacy proposal credit negative for linear TV and wireless providers – Over half a trillion in rated debt affected*."

Moody's clearly explains how applying rules unequally, requiring ISPs to get consumer permission to use data for advertising that Google, Facebook and edge advertisers do not have to get permission to use, creates unequal protection for users' privacy and starkly unequal opportunity to fairly compete for digital advertising revenues going forward.

Moody's **explained**:

"*We believe this proposal will have a negative impact on both fixed and mobile broadband providers. If approved,* ***the ability to compete*** *with digital advertisers such as Facebook and Google (Aa2 stable), who are able to collect the same type of data from consumers who access their websites and those of others,* ***will be severely handicapped in the future*** *as the old guard ecosystem evolves to become more competitive. We believe this to be a* ***long-term risk to the current TV advertising business model, as well as all broadband providers whom also have ad sales exposure to the present linear video ecosystem****… An open question is how this proposal may impact the FCC's other recent proposal regarding unbundling the provision of the set top box from the ISP, which is* ***also negative for broadband providers****…"*

"Absent an alignment of rules between the FTC and FCC regarding these privacy laws, ***a distinct competitive advantage will be given to online digital advertisers****…"*

"The FCC's proposal also has the ***potential to derail efforts by wireless carriers to cultivate mobile video advertising revenues****. Wireless carriers have the potential to generate significant advertising revenues due to their ability to precisely target ads to wireless subscribers. But,* ***if the FCC restricts the carriers' ability to collect this data, the advertising revenue opportunity will be reduced. Without a robust mobile video advertising market, the product could lose relevance due*** *to its higher cost to consumers and a potential for fewer content choices*." [**bold** added for emphasis].

3 Takeaways from Moody's Analysis of the FCC's unequal ISP privacy policy

First, it spotlights the FCC's unequal consumer privacy protection policy, because the information the FCC is regulating is not private-protected information to anyone but ISPs, who are the only entities in the U.S. that have to treat this otherwise non-private information privately by getting a consumer's permission for the ISP to use it for advertising.

Second, its spotlights the FCC's unequal competitive opportunity policy. Every business in America that is not an ISP can use a consumer's FCC private information without their permission to serve them ads or offer them new personalized products and services, while the FCC applies its purported "permissionless innovation" policy in an unequal manner that arbitrarily limits only ISPs to permission-dependent innovation.

Third, it effectively debunks the FCC's claim that its reclassification of broadband ISP service has no effect on broadband investment. **Moody's Investor Service** is one of the leading credit and risk analysis

providers in the world, and they clearly see the FCC Title II privacy policy as "credit negative" or bad for investment for the half of trillion dollars in U.S. broadband ISP debt.

They also clearly explain how the U.S. broadband providers' businesses and competitive opportunity are at a distinct competitive disadvantage to Google, Facebook and other edge digital platform providers. The FCC needs to rethink its silly claim that unequal "strongest possible" utility regulations don't adversely affect infrastructure investment.

Overall, it is critical to remember that the FCC staff and Chairman originally did not want Title II reclassification and by extension, Title II section 222 privacy policies, to only apply to ISPs in the Open Internet order.

Remember that this unequal protection and unequal opportunity legal positions were a direct result of an arbitrary, self-serving, eleventh-hour **ex parte** from Google that pressured the FCC to reject as wrong Judge Tatel's entire understanding and legal analysis of common carrier service in his ***Verizon v. FCC*** decision.

In ***Verizon v. FCC*** Judge Tatel described an obvious implicit service between a broadband provider and an edge provider like Google as a potential Title II telecommunications service. The Google ex parte directly challenged Judge Tatel's common carrier legal expertise by repeatedly dismissing the existence of the service Judge Tatel described by calling it an: "*imagined edge provider access service*"… "*a non-existent edge provider service*"… and "*without reference to any evidence, that "broadband providers furnish a service to edge providers"*…"

If the FCC had not been politically forced to adopt Google's self-serving legal analysis to self-exclude Google's dominant edge platform service from Title II classification, the FCC's Title II ISP privacy NPRM would not have created unequal protection for consumers or unequal opportunity for competitors.

***

5. PrecursorBlog: Why Is the FCC Regulating the Biggest Privacy Risk Platforms the Least?

Submitted by Scott Cleland on Fri, 2016-04-29 11:01

The epic flaw in the FCC's Title II privacy NPRM is that it purports to best protect consumers' private information by only regulating broadband providers' use of that private information, while emphatically protecting dominant edge platforms from FCC privacy regulation when they use that same FCC-regulated private information indiscriminately without consumers' meaningful knowledge or consent.

Yes you read that right.

Apparently the FCC thinks it is more important to protect dominant edge platforms from FCC privacy regulation, than it is to protect consumers' private information.

The issue of privacy lays bare the FCC's contorted and arbitrary logic of both its Title II cleave that only ISPs can be gatekeepers, and that the goal of net neutrality, protecting dominant edge platforms from ISP interference, is logical and appropriate to apply to privacy. If it was, that would perversely mean that the purpose of the FCC's privacy rules should be to protect edge providers' businesses, not consumers' privacy.

If you want to see a visual representation of this problem, please see the attached one-page graphic **here**.

It visually exposes the illogic and hypocrisy in the FCC regulating only ISPs on privacy and not edge platforms, when several #1 edge platforms are dominant in several markets, with much more national market share than the #1 ISPs in their markets.

This is a wrong policy because the edge platforms have much more gatekeeper power and much more private data collection opportunity than ISPs do.

First, based on StatCounter's market share data in the U.S. please consider the following.

Google dominates the following markets, mobile search, desktop search, and desktop browser, with 91%, 79%, and 50% U.S. market shares respectively.

Facebook dominates social with 79% share.

Microsoft dominates desktop OS with 78% share.

And Apple leads the following markets, device manufacturing, mobile OS and mobile browser with 58%, 58%, and 55% U.S. market shares respectively.

In stark contrast, the number one ISPs in fixed and mobile broadband respectively, Comcast and Verizon, each have U.S. market shares of ~33% of their respective markets, based on FCC and company report data.

Simply, this shows that these dominant edge providers have at least 50% to 175% more "gatekeeper" power that the top ISPs do, and dramatically more gatekeeper power than that of any other ISP.

Moreover, the FCC is well aware that ISPs are limited by antitrust precedent and the FCC's media ownership rules to about a third of a market supposedly because of "network effects," while the dominant edge providers have been able to become dominant precisely because they have no practical antitrust/FCC limit on their scale, scope or reach, and because they enjoy phenomenal inter-network effects that the world has never seen before.

So who are the real gatekeepers? Edge platforms are the real gatekeepers because they have been allowed to gain unprecedented scale, scope and reach.

Second, this chart shows the positioning of these dominant edge platforms. They are in between the users' device and the ISP. Thus these entities don't rely on an ISP for consumers to use these services because users' devices enable these applications before the ISP is ever involved.

Moreover, if Google, Apple, Facebook and Microsoft encrypt their traffic, as they are doing and plan to do more universally, over 90% of traffic coming from these dominant edge platforms will either be dark/unintelligible to the ISP, or invisible because it is rerouted to edge proxy ISP servers that do the encrypting.

Some will claim that ISPs are different from edge platforms because of higher switching costs. Google deceptively claims "competition is a click away." That may be truth, but not the whole truth and nothing but the truth.

Think about it. If a user wanted to totally switch from all Google's or Facebook's products and services, there would be huge switching costs. Leaving Google or Facebook *completely* like one completely would leave an ISP, would obviously take much more *personal* time and *personal* effort and *personal* hassle than switching an ISP, and that doesn't even touch the inefficiencies of trying to reconstruct a Google-like integrated service without Google, or a Facebook-like connected/networked service without Facebook.

In sum, the FCC has put itself in a largely indefensible position.

It is claiming that it must protect certain private information from being used without permission by ISPs while at the same time the FCC is going out of its way to ensure that edge platforms, that have vastly more gatekeeper power than any ISP, and that Hoover-up private information indiscriminately for a living without the meaningful knowledge or consent of their users, are protected from the FCC's Internet privacy regulations!

These proposed privacy regulations lay bare that the FCC is more committed to protecting dominant edge providers' commercial interests, than American consumers' privacy interests.

***

6. Precursorblog: Goobris: Google Expecting Less Privacy Regulation than its Competitors

Submitted by Scott Cleland on Tue, 2016-05-10 10:43

Why does the company that by far collects the most private information that the FCC claims it wants to protect, and that also has the worst consumer privacy protection **record** with the FTC, (Google), get 99% exempted from the telecom and cable privacy protections expected of telephone, broadband, cable and satellite providers?

Is it the same reason, that the edge platforms with much more gatekeeper power and private data collection opportunity than ISPs somehow warrant no FCC privacy regulation? (See info-graphic **here**; explanation **here**.)

How can the U.S. credibly demand a data safe harbor in the EU on the basis of promises that the U.S. has vigilant, robust and comprehensive privacy enforcement in the U.S., when the worst privacy offender in both Europe and the U.S., Google, de facto enjoys special lenient privacy treatment from both the current FTC and the current FCC?

Those are good questions for the Senate Judiciary Committee to ask FCC and FTC leadership this week at its privacy oversight hearing, which in part is examining why the FCC and FTC appear more interested in protecting Google and other Big Internet companies from privacy regulation, than in protecting consumers' expected communications and viewing habits privacy.

What are the facts?

Google collects and stores vastly more private information than any other entity – see the evidence **here**. Google also has the worst privacy record of any major American company – see the evidence **here**. Google's dominant mobile operating system, Android, also has the worst data protection record of any major American company – see evidence **here**. To understand why Google is a uniquely problematic privacy problem, see the detailed analysis and evidence **here**.

Google serves **~3x times** more Americans than any ISP. Google currently **boasts** that YouTube has a larger primetime viewing audience than the top ten U.S. TV shows combined.

Google **collects** vastly more private information than any ISP: IP addresses via Search, Analytics, Cookies, & Chrome; Email addresses via Gmail scanning & Postini filters; WiFi, SSID & MAC addresses via WiFi war-driving; Phone/mobile #s via Play, search, Android, Voice, Talk; Voiceprint recognition: via Hangouts, Translate, YouTube; Face-print recognition via Google+, Photos, YouTube; 103 Languages identified via Translate, Voice, Video; Home info: via Maps, Earth, StreetView, Android, Play; personal info via Account, apps, product, service registrations; Social Security, passport &license #s via Desktop Search; Credit card & bank info: Checkout, Shopping, & Wallet; Health identifiers by Search, Google+, Gmail, News, Books; and Click-print IDs via analysis of multiple web histories.

Where is the special treatment of Google?

Concerning the FCC's Title II Section 222 privacy rules that apply to telecommunications, a week before the FCC voted on the Open Internet order, Google submitted an **ex parte recommendation** to the FCC, that the FCC adopted, that said both the FCC and the ***Verizon v. FCC*** court were wrong in their understanding of telecommunications. This last minute legal interpretation whipsaw, meant Google politically exempted itself not only from Title II Section 222 privacy rules, but also exempted itself from CALEA responsibilities to cooperate with law enforcement investigations.

Concerning the privacy rules for the AllVid set-top box proceeding, Google's **comments** claimed special treatment in so far as they urge the FCC to not apply cable and satellite viewing-habit privacy

regulations to over the top video like Google. Effectively Google is rejecting the overwhelming bipartisan votes in 1992 and again in 2004 for ensuring that consumers' video viewing habits were private not public information.

Google's AllVid comments to the FCC also glistened and wafted in "Goobris," (defined as hubris to the Google power), in telling the FCC that it did not need to try and regulate Google because "*the robust privacy and data security protections that already apply at the federal and state levels will continue to protect consumers*."

Some context is essential to grasp the full extent of Goobris here.

Concerning State law enforcement, let's not forget that for over a year during 2015 and 2016, Google secured a Federal Court injunction that effectively prevented any state law enforcement authority from even *investigating* an alleged Google violation of any state consumer protection law, including state privacy laws. For those shaking their head in disbelief how such a perverse outcome could or did happen, **here** is the documentation and explanation of this dark period in state law enforcement vis-á-vis Google.

Concerning FTC law enforcement vis-á-vis Google, let's not forget that since the FTC abruptly and suspiciously dropped all FTC antitrust charges against Google in January 2013, including its Android investigation without a peep, the FTC has not enforced privacy law against Google.

That is remarkable because Google is the only company that sufficiently violated the FTC's privacy policy to warrant a twenty-year, FTC-Google-Buzz privacy order, AND also seriously violated it within the first year, resulting in a settlement and the **highest FTC privacy fine ever**, $22m, for hacking into Apple's iPhones to change consumers' privacy and security settings to allow Google to track and advertise without consumers knowledge and consent.

Making matters worse, since then, the FTC has ignored **repeated charges and evidence** that Google has further violated its FTC-Google-Buzz privacy order.

A December 2015 **EFF petition and complaint** to the FTC charged that Google violated its promise to protect students' privacy in publicly signing the Student Privacy Pledge. To date the FTC has done nothing.

It gets worse.

The FTC has known of Google Apps for Education serious privacy problems for almost two years with no action.

In March 2014, Education Week **reported** that Google was **exposed** in a civil suit deposition to have secretly read all student-Gmail before it was received without any notice or "informed consent," for the commercial purpose of creating a targeted advertising profile on the student for the future. In an April 2014 mea culpa **blog post**, Google effectively had to admit that for three years until April 29th 2014, Google secretly had been illegally collecting private student data for advertising purposes in violation of

their public privacy representations and FERPA. The analysis **here** by world-leading privacy advocate Simon Davies explains why this three-years-late, Google privacy invasion disclosure affecting minors is especially serious, inadequate and misleading.

In short, Congressional overseers should question how the FTC and FCC can defend the least privacy regulation/enforcement of the worst consumer privacy violator?

And also ask why consumers' privacy interests overall, have apparently been subordinated to Google's corporate interests?

***

7. PrecursorBlog: Google's Omnipresent Tracking Much Harder to Leave than an ISP for Privacy

Submitted by Scott Cleland on Tue, 2016-05-17 09:20

If you are online, you can't escape Google's myriad of ways it tracks you, but you can leave your ISP.

A famous 2009 Google Blog **post** boasted that: "*Google is not the Hotel California — you can check out any time you like and you CAN, in fact, leave!*"

Since Google chose that apt metaphor, and boasted about how easy Google makes it to "*check out*" your private data and "*leave*" to a competitor, lets test if you can ever "*in fact leave*" Google-Eye's pervasively invasive online surveillance -- from a privacy perspective.

But first, why is this point a relevant exercise for people who care about privacy at this particular point in time?

Right now in the U.S., the FCC is trying to **justify differential treatment of ISPs and dominant edge platforms like Google** in its Title II privacy proceeding and its AllVid set top box proceeding, by claiming that ISPs are more "sticky" and harder to leave than dominant edge platforms like Google.

The Senate Judiciary Committee last week **heard** testimony from the FCC that: *"…we can choose not to visit a website or not to sign up for a social network, or we can choose to drop one and switch to another in milliseconds. But broadband service is fundamentally different. Once we subscribe to an ISP—for our home or for our smartphone—most of us have little flexibility to change our mind or to do so quickly.*"

The FCC Chairman also **said**: "*I go to WebMD, and WebMD collects information on me. I go to Weather.com, and Weather.com collects information on me," he said. "I go to Facebook, and Facebook collects information on me. But only one entity collects all of that information, that I'm going to all of those different sites, and can turn around and monetize it*."

I don't challenge that there is a real time hassle to switch ISPs.

What I do respectfully challenge is that first, Google essentially doesn't "*collect all of that information*" because they do (see **here**), and second, that Google somehow is easy to escape, **when it comes to collecting one's private information**, because it is not, as I will prove below.

Let's return to Google as a "Hotel California" where "you can check out but never leave."

Google likes to present the mirage of freedom by touting that they allow users to leave by easily exporting their private information to take elsewhere. As with most things Google, that's the truth, but not the whole truth and nothing but the truth.

One can take a copy of one's data, and leave, but Google generally retains a copy of it all and can use it for all sorts of purposes. Tellingly, Google's Cloud Platform director Tom Kershaw **told** the New York Times last year: "*Never delete anything, always use data – it's what Google does…"*

Most importantly, when you leave Google, it can still track most all you do. How?

First, if you surf the web, you need to know that **~98%** of the top ~15 million websites use Google Analytics so most everywhere you go on the net, Google can track you.

Second, **two million** of the most popular websites use the Google YouTube Display Ad Network to serve you video and other display ads so they can track you.

Third, **1.2 million** of the top websites about physical locations like stores, restaurants, hotels etc. have Google Maps embedded by default enabling Google to track your location and intent.

Fourth, even if you are not one of the billion plus Gmail users, **Google's Gmail algorithm secretly reads your emails** that are sent to Gmail users.

Finally, if you use any type of smartphone **93%** of all mobile searches use Google Search because it is installed by default by manufacturers on Android and Apple smartphones/tablets, and if you are the half of U.S. users who use Android, the dominant licensable operating system in the U.S., multiple Google mobile services track your usage and location in order to function as designed.

In sum, if you are a consumer who values their privacy and seeks to control the use of their private information, it is likely a more involved ongoing hassle to quit all Google services and avoid Google's ongoing pervasive tracking of non-Google users, than it is to leave an ISP.

That's because once the time hassle of leaving your ISP is done, the privacy concern is done. However, if one tries to leave Google-Eye's persistent surveillance, the hassle and switching cost of proactively protecting one's private information from Google is not over, it persists indefinitely.

If you want to learn about all the things one has to do to fully quit Google's omnifarious products and services, see these accounts of what it involves to leave Google completely from: **Slate**, **TechRepublic**, **ieee.org**, **MacWorld**, **PCWorld**, **Time**, and **MakeUseOf.com**.

Simply, with Google you may be able to check out, but when you think you've left them, they still secretly follow you most wherever you go online.

***

Scott Cleland served as Deputy U.S. Coordinator for International Communications & Information Policy in the George H. W. Bush Administration. He is President of Precursor LLC, an emergent enterprise risk consultancy for Fortune 500 companies, some of which are Google competitors, and Chairman of NetCompetition, a pro-competition e-forum supported by broadband interests. He is also author of "Search & Destroy: Why You Can't Trust Google Inc." Cleland has testified before both the Senate and House antitrust subcommittees on Google and also before the relevant House oversight subcommittee on Google's privacy problems.

Scott Cleland
Precursor LLC
202-828-7800
Scleland@precursor.com